

| NODIS Library | Legal Policies(2000s) | Search |



NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A
Effective Date: May
16, 2006
Expiration Date: May
16, 2011

[Printable Format \(PDF\)](#)

[Request Notification of Change](#) (NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [Chapter5](#) |
[Chapter6](#) | [Chapter7](#) | [Chapter8](#) | [Chapter9](#) | [Chapter10](#) | [Chapter11](#) |
[Chapter12](#) | [Chapter13](#) | [Chapter14](#) | [Chapter15](#) | [Chapter16](#) | [Chapter17](#) |
[Chapter18](#) | [Chapter19](#) | [Chapter20](#) | [Chapter21](#) | [AppendixA](#) | [AppendixB](#) |
[ALL](#) |

Chapter 21 Audit Trails and Accountability

21.1 Audit Trails and Accountability Overview

21.1.1 An audit trail is a series of records of IT events about a user, an application, or an operating system. Audit trails are designed to capture and maintain a record of system activity.

21.1.2 The NASA ITS Program requires that audit trails, used in conjunction with the appropriate tools and procedures, shall be collected and utilized for individual accountability, reconstruction of events, intrusion detection, and problem identification.

21.2 Audit Trail and Accountability Requirements

21.2.1 NASA shall ensure that all audit trail and accountability requirements identified in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, have been implemented.

21.2.2 NASA shall ensure that:

- a. Audit trails are implemented on all NASA IT systems. The amount of detail logged shall be commensurate with the system's information category and impact level.
- b. The confidentiality of the audit trail information is protected as ACI or SBU, according to the guidelines in NPR 1600.1, NASA Security Program Procedural Requirements.

- c. Audit trails are reviewed periodically, with the frequency of these reviews and retention schedules being consistent with the security category of the system.
- d. Access to on-line audit logs is strictly controlled.
- e. There is a separation of duties between security personnel who administer the access control function and those who administer the audit trail. This is a requirement for high and moderate impact systems and strongly recommended for low impact systems.

21.3 Additional Audit Trail and Accountability References

- a. NIST SP 800-12, Introduction to Computer Security: The NIST Handbook.
- b. NIST SP 800-31, Intrusion Detection Systems.

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) |
[Chapter5](#) | [Chapter6](#) | [Chapter7](#) | [Chapter8](#) | [Chapter9](#) | [Chapter10](#) |
[Chapter11](#) | [Chapter12](#) | [Chapter13](#) | [Chapter14](#) | [Chapter15](#) |
[Chapter16](#) | [Chapter17](#) | [Chapter18](#) | [Chapter19](#) | [Chapter20](#) |
[Chapter21](#) | [AppendixA](#) | [AppendixB](#) | [ALL](#) |

| [NODIS Library](#) | [Legal Policies\(2000s\)](#) | [Search](#) |

DISTRIBUTION: **NODIS**

This Document Is Uncontrolled When Printed.

Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
